Quiz 7 Solutions

written by Alvin Wan . alvinwan.com/cs70

Wednesday, September 28, 2016

This quiz does not count towards your grade. It exists to simply gauge your understanding. Treat this as though it were a portion of your midterm or final exam.

1 RSA

1. **Prove or Disprove**: Given two different public keys, N_1 and N_2, $d = \gcd(N_1, N_2)$ cannot be composite.

   Solution: Assume for contradiction that d is composite. Since N_1 and N_2 are each made of only two primes each, and d is a common factor for both N_i, then d is the product of two primes. We now have two cases:

   (a) Since d contains two primes and each N_i contains exactly two primes, $d = N_1$ and $d = N_2$. This means $N_1 = N_2$. However, $N_1 \neq N_2$. Contradiction.

   (b) $d \neq N_1$. However, d is a factor of N_1. Since d has two primes and $N_1 \neq d$, then N_1 is composed of at least three primes. Contradiction. (Remember, we know that in RSA, N is the product of exactly two primes.)

2. **Prove or Disprove** There are finitely many polynomials in $\mod p$ for some prime p. (If true, find an expression for the number of polynomials. If false, prove the opposite.)

   Solution: In mod p, there are p possible numbers. By Fermat's Little Theorem ($a^p \equiv a \mod p$), we see that the maximum degree for any polynomial is $p-1$. Note that we cannot apply $a^{p-1} \equiv 1 \mod p$ because a could be 0. This means that the maximum number of terms is p, where each has p possible coefficients. This makes p^p possible polynomials in mod p.